IN THE SPECIFICATION:

Please replace the Abstract of the Disclosure appearing on pages 66 and 67 of the specification, with the following amended Abstract of the Disclosure:

-- The present invention is directed to computer networks and more particularly to a system and method in a network device for caching Hyper Text Transfer Protocol (HTTP) data transported in an Internet Protocol (IP) Datagram sent on a socks connection established over a Transmission Control Protocol (TCP) connection between a source port on a source device and a destination port on a destination device. ~~The method comprises the steps of:~~

~~identifying the source device, the destination device, the port on the source device, the port on the destination device of an incoming IP Datagram.~~

~~determining whether the incoming IP datagram is originated by a socks client or by a socks server :~~

~~If the incoming IP Datagram is originated by a socks client:~~

~~terminating the TCP connection and the socks connection ;~~

~~identifying the socks connection in a table;~~

~~identifying the application level protocol associated with the socks connection referring to this table, this table comprising for each socks connection an application level protocol;~~

~~determining whether said application level protocol is HTTP or not:~~

~~If said application level protocol is HTTP:~~

~~determining whether HTTP data requested by the incoming IP Datagram is in a local cache within the network device or not:~~

~~If HTTP data requested by the incoming IP Datagram is in a local cache:~~

~~building an outgoing IP Datagram comprising requested HTTP data retrieved from the local cache;~~

~~sending said outgoing IP Datagram to the socks client originator of the incoming IP Datagram.~~ --

Please replace the paragraph appearing on page 8, lines 6-15 of the specification, with the following amended paragraph:

-- HTTP is an Application Level protocol used by the TCP connections between WEB Browsers and HTTP Proxy Servers. Consequently, IP Datagrams exchanged between the WEB Browsers and HTTP Proxy Servers comprises HTTP data. Since HTTP Proxy Servers manage the HTTP connections, they see and handle the HTTP data comprised in the IP Datagrams. When a HTTP Proxy Server receives from a source system (a WEB Browser) a request to retrieve HTTP data (a WEB page) located on a destination system (a WEB server), two situations can occur depending on whether the requested HTTP data is already stored in a local cache, or not. --

Please replace the paragraph appearing on page 10, lines 10-24 of the specification, with the following amended paragraph:

-- Socks Servers are used within an Intranet to provide secure access to systems located outside the Intranet. The Socks protocol is a form of encapsulation of Application Level traffic such as HTTP, FTP, Telnet. The Socks protocol (and not HTTP) is the protocol used by TCP connections established within the Intranet between WEB Browsers and Socks Servers. Consequently, IP Datagrams exchanged between WEB Browsers and Socks Servers comprise Socks data. In a Socks environment, IP routers and network devices within the Intranet only see and handle Socks traffic. As a consequence, all Application Level protocols (including HTTP) encapsulated by Socks are not seen and are therefore not processed by any IP router and more generally by any network device within the TCP/IP network. Since HTTP data transported in IP Datagrams data are not seen by IP routers in a Socks environment, IP routers cannot [[not]] cache said HTTP data. --

Please replace the paragraph appearing on page 25, lines 17-20 of the specification, with the following amended paragraph:

--

- (601) Socks Connection table. This table comprises for each Inbound Socks connection the identifier of the Outbound Socks connection and the Application Level protocol. This internal table [[are]] is detailed in Figure 6. --